

# Monitoring of international legal regulation trends aimed at development of legislation in digital economy in Russia

## **Restricting movement of autonomous vehicles on public roads, special measures to protect children in the digital environment**

*Monitoring No.4 (April 2024)*

**Monitoring** was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):

*Antonina Levashenko*, Senior Researcher, International Best Practices Analysis Department at the Gaidar Institute;

*Maria Girich*, Researcher, International Best Practices Analysis Department, Gaidar Institute.

*Ivan Ermokhin*, Researcher, International Best Practices Analysis Department, Gaidar Institute.

*Olga Magomedova*, Researcher, International Best Practices Analysis Department, Gaidar Institute;

*Tatiana Malinina*, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute

*The reference to this publication is mandatory if you intend to use this material in whole or in part.*

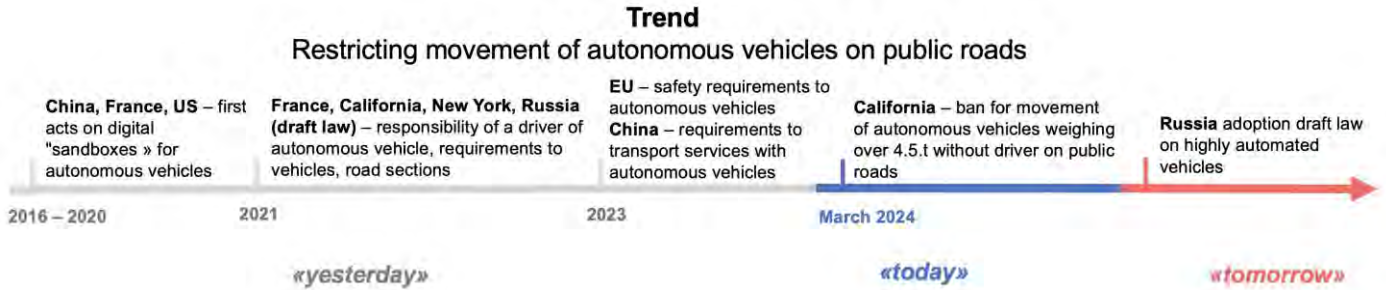
*"I know how to talk short about long stuff"*

*Anton Chekhov*

In April 2024, two events can be highlighted that define trends in the development of digital economy regulating.

**Trend No.1. Restricting movement of autonomous vehicles on public roads**

In April 2024, California (USA) proposed to completely restrict movement of autonomous vehicles (hereinafter referred to as "AVs") weighing more than 4.5 tons on public roads. A number of other countries (China, France) allow movement of such vehicles, but under license and compliance with safety requirements for road sections, etc.



**Trend No.2. Special measures to protect children in digital environment**

In April 2024, the UK, Brazil and the US simultaneously adopted a number of measures to protect children and young people in the digital environment. Since the beginning of 2024, China and Singapore have already adopted some of them. These measures apply to both users and operators providing online services, including platforms and social networks, and manifested the increased regulation: measures against cyberbullying, monitoring time of using digital products and minimizing collection and dissemination of children's personal data.



# Key aspects

## 1. Restricting movement of unmanned vehicles on public roads

In April 2024, a bill was proposed in California to restrict movement of vehicles weighing more than 4.5 tons without drivers on public roads (vans and heavier trucks). This bill is promoted by a trade union of truck drivers, who risk losing their job due to use of unmanned trucks.

In France, movement of such unmanned vehicles is allowed only on special roads, in China - in presence of a remote operator, in most states of the USA such a vehicle can be denied permission to move.

The OECD and ITF<sup>1</sup> use classification of the automated transport vehicles highlighting 6 levels.<sup>2</sup> The level of automation determines who takes control on driving from partial automation (level 0) to full automated unmanned driving on any roads (level 5). In the EU, as from 2024 all new vehicles shall be equipped with advanced emergency braking systems and keeping the lane of traffic, which makes it virtually impossible to purchase a new car without automation level 1.

### The experience of EU, US, China and France

The general trend is to develop safety requirements for Level 3 and 4 unmanned

vehicles and higher standards for Level 5 vehicles:

1) Compliance with technical requirements for systems that replace driver control, i.e. signaling, steering, acceleration and braking (EU, California, France);

2) Real-time information systems on the state of the vehicle and the surrounding area (EU, France). In France, such data are used to analyze accidents, and the manufacturer of the automated vehicle is obliged to provide access to the data;

3) Driver monitoring system to assess whether the driver is able to take control of the vehicle, e.g. in case of risk of an accident (EU, France, California, Nevada). If a driver does not react, the vehicle must stop (California);

4) Defining conditions by manufacturer (geographical, weather, road, etc.) for unmanned driving (France);

5) Defining conditions for the automated system of the vehicle to activate an emergency maneuver in case of a risk of collision (France).

In this respect, in the EU, for Level 5 vehicles there is a requirement to have data recorders of events related to the movement of the vehicle (route, barriers, accident risks, driving data, etc.), systems for informing about safety of other road users (e.g. driver absence);

Level	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
<b>Control function</b>	driver operates the vehicle, special functions are automated			driver controls vehicle only if the vehicle requests	fully automated driving, driver may be absent	
	<b>Functions of driver's support</b>			<b>Functions of automated driving</b>		
<b>How functions are realized?</b>	Issuance of warnings and immediate aid to driver	steering OR braking accelerating aid	steering AND braking accelerating aid	driver controls vehicle if vehicle requests	automated driving in any condition	
<b>Examples</b>	- automated panic braking - lane departure alert	- lane centering OR - adaptive cruise control	- lane centering AND - adaptive cruise control	automation while driving	- driving on dedicated roads - pedals and steering wheel may be missing	similar to level 4, but vehicle may move without driver on any roads

Table – 6 levels of vehicle’s automation

<sup>1</sup> International Transport Forum

<sup>2</sup> <https://www.itf-oecd.org/sites/default/files/docs/preparing-infrastructure-automated-vehicles.pdf>

6) Switching on/off mechanism for automated driving (New York, Nevada);

7) Compliance with regulations to protect against cyberattacks, unauthorized intrusions and false commands (California, New York). In California, a vehicle must be equipped with a separate mechanism to collect and store data 30 seconds before hitting anything.

8) Marking of autonomous vehicles (China);

It is worth noting that China's approach is somewhat different from other countries. It provides for licensing of public passenger transport and freight transport services provided using vehicles of 3-5 levels of automation.

It is worth noting that China's approach is slightly different from other countries. It provides for licensing of public passenger transport and freight transport services provided using vehicles having 3-5 levels of automation. The operator should implement an operational security management system, including employee safety, threat investigation, network security management, and emergency response plans.

In order to enter such vehicles on the roads, countries impose the following conditions:

- 1) Highly or fully automated vehicles must drive only on specially dedicated lanes or routes (France, China), or the manufacturer must obtain a permission to use automated vehicles on public roads (US states).

In France, they appoint a special operator of such routes, who organizes the route, conducts a safety assessment of the route with authorized organizations, and obtains permission from the prefect to put the route into operation. In California and Nevada there are no dedicated roads for automated vehicles, however, manufacturers must obtain a permission to operationalize such vehicles on public roads (there may be a requirement for compulsory presence of a driver).

In China, at least an operator (driver or someone in charge of safety) must be present in autonomous vehicles, such as cargo autonomous vehicles, during transportation, and fully automated taxis can be used without drivers with the permission of local authorities in specially allocated places, however, using a

remote control. One operator cannot control more than 3 vehicles;

2) The manufacturer must test an automated vehicles on public roads (California, New York, Nevada).

In China, the operator of autonomous vehicles is required to establish a transportation safety guarantee system before operating the vehicle, for example, by signing an agreement with manufacturers, safety inspectors, etc.;

3) The manufacturer must have \$5 mln or more in insurance (California, Nevada, New York).

There are also requirements for road systems/lanes that are used for automated vehicle traffic:

1) Road systems/lanes must be designed to avoid accidents (France). New York demands a certificate from the vehicle designer to certify that the automated vehicle will be safer than a human driver;

2) There must be systems to detect malfunctions, risks of moving beyond the boundaries of the designated road, and informing the operator (France);

3) In case of an accident, there shall be an analysis of all risks and reasons of the accident (France, California, New York).

In France, all road accidents shall be reported by the system operator to the prefect, in New York and California (bill) by vehicle manufacturers to the state road authorities;

4) There shall be an annual safety audit (France).

As for liability of the person driving the vehicle, in France the driver is not criminally liable for offenses if the vehicle is operated by an automated system (for levels 3 to 5).

A driver is liable for an accident if: (1) assumes control of the vehicle; (2) fails to assume control of the vehicle when requested by the automated system; (3) the driver fails to comply with law enforcement orders. Being under the influence of alcohol is also penalized. A similar liability regime is proposed by California in April 2024.

China has adopted liability rules within the Shenzhen<sup>3</sup> Special Economic Zone: (1) if the vehicle is driven by a driver, the driver is liable for the accident; (2) if there is no driver, the owner or manager (operator) of the vehicle is

<sup>3</sup> Правила управления интеллектуальными подключенными ТС 2022 г.

liable. If the vehicle caused damage due to a defect, the driver (owner or operator) pays compensation to the victim, and then, they are entitled to claim compensation from the seller, manufacturer or dealer of the vehicle.

### Russia's experience

Russia has twice proposed laws on HAVs (highly automated vehicles) in 2021 and 2022 (today there is only regulation acting in respect of experimental legal regimes).

Under draft laws, it was proposed to place the responsibility for road traffic accidents on the HAV's owner with the burden of proving the absence of fault or the fault of other participants (operator, developer, dealer) was also placed on the HAV's owner. In the US states and France, the driver is not liable if the vehicle was being driven by an automated system at the time of the accident. The Ministry of Transport stated that it would prepare updates to the draft law in 2024.

The RF Government Decree of 09.03.2022 No.309 (experimental legal regime for HAVs) also states safety measures: HAV's must include a control system that enforces traffic rules, monitors traffic conditions, interacts safely and predictably with other road users, can diagnose its own malfunctions, etc. For each HAV the risk of liability for harm to life, health or property of other persons shall be insured for RUR 10 mln under experimental legal regime (ELR).

The HAV's owner (operator) under the ELR is obliged to conduct continuous remote monitoring, if the HAV is moving without a driver in the cabin (only with remote routing and dispatching), level 4 of vehicle automation is regulated.

Thus, Russia has a limited ELR regulation allowing to drive on dedicated roads without a driver subject to remote monitoring of the vehicle. In foreign countries, the driver is liable for the accident (there are cases of exclusion of liability), then, like in Russia, the owner of the vehicle (or manufacturer is liable for

misinformation). However, it is not clear, whether the dispatcher will be liable (controls the vehicle remotely) or the dealer (HAV's technical check-up and maintenance), if the accident was due to their fault.

## 2. Special measures to protect children in digital environment

### Experience of UK, US, China, Singapore, and EU

In April 2024, UK published priorities for 2024-2025 on protection of children personal data in the digital environment<sup>4</sup>, and the US has a draft of Children's Online Privacy Protection Act<sup>5</sup>, (another bill was introduced in March)<sup>6</sup>; Brazil approved a Decree on the Rights of Children and Adolescents in the Digital Environment.<sup>7</sup> Moreover, in January 2024, China's<sup>8</sup> online child protection regulations came into force, and Singapore adopted guidelines on the protection of children's personal data in the digital environment<sup>9</sup> in March 2024. Thus, there is a trend towards greater protection in the digital environment for children by clarifying regulatory measures.

These measures demonstrate an expansion of the scope of regulation in part of:

a) age of users (USA, Singapore, China, France). For example, age verification, restriction to online services/social networks based on age, restriction of personal data collection;

b) products: one bill in the U.S. proposes to extend the duty to protect minors to online and mobile app providers.

Measures in various countries and regions are broadly similar and include:

1. Prohibited (e.g. involving children in increasing online service traffic - UK, USA, China) and restricted practices (e.g. displaying unhealthy content - UK, China; targeted advertising - UK, USA; controlling service usage time - China, France).

However, approaches to implementing restrictions vary from prohibitive in China to

<sup>4</sup> <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-sets-out-priorities-to-protect-childrens-privacy-online/>

<sup>5</sup> <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-sets-out-priorities-to-protect-childrens-privacy-online/>

<sup>6</sup> <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-sets-out-priorities-to-protect-childrens-privacy-online/>

<sup>7</sup> <https://www.loc.gov/item/global-legal-monitor/2024-04-14/brazil-rights-of-children-and-adolescents-in-digital-environments-regulated/>

<sup>8</sup> [https://english.www.gov.cn/policies/latestreleases/202310/24/content\\_WS6537a5d2c6d0868f4e8e095e.html](https://english.www.gov.cn/policies/latestreleases/202310/24/content_WS6537a5d2c6d0868f4e8e095e.html)

<sup>9</sup> [https://english.www.gov.cn/policies/latestreleases/202310/24/content\\_WS6537a5d2c6d0868f4e8e095e.html](https://english.www.gov.cn/policies/latestreleases/202310/24/content_WS6537a5d2c6d0868f4e8e095e.html)

relatively lenient in Europe and the United States. For example, in China, the use of online games is limited to specific times (e.g., weekends), while in France a system is envisioned that regularly notifies the user of the duration of social network operation. In the EU, it is prohibited to use children's data for personalized advertising.

Approaches to parental control also differ: in China it is mandatory for online audio and video services and social networks, whereas in the UK it is an option where the provider must inform the child;

2. Higher standards towards confidentiality, etc.:

a) Data protection is embedded at the product design stage (UK, Singapore, China, EU plans);

b) Assessing the impact of online protection (UK, China), risks of child rights violations (EU) - e.g. what information is collected and exactly how it is used;

c) Protection of children's data should extend not only to products designed specifically for children, but also to other products to which children have real access, i.e., social networks, EdTech, online games (USA, Singapore);

d) Disabling geolocation by default, to limit the ability to determine the child's location, e.g. on social networks (UK, US, Singapore);

e) Age-appropriate language for using information about users' data (UK, Singapore);

f) The age to submit data to online services is usually 13, but in Singapore operators can set a higher age threshold, and in France it is 15 for social media accounts<sup>10</sup>;

3. Increased requirements to data security, including minimization of collection and dissemination of minors' data (UK, USA, Singapore, China), possibility to change and delete such data (USA, China).

### Russia's experience

In Russia, the Law "On Protection of Children from Information Harmful to their Health and Development" prohibits dissemination of information among children that incites harm to health or life, encourages participation in gambling, and justifies violence and cruelty.

Certain information, for example, causing fear or panic, is restricted to age categories. These requirements apply to Internet. At the same time, measures to protect children are broader than restrictions on the dissemination of information, and in this sense, Russia lags behind the most significant global trends. For example, there are no measures against cyberbullying, tracking children through geolocation (e.g., disabling geolocation for children's social media accounts).

<sup>10</sup> <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>